DOCUMENT RESUME

ED 332 689 IR 015 034

AUTHOR Johnson, Dell
TITLE The Future of Electronic Educational Networks: Some Ethical Issues.
PUB DATE May 91
NOTE 15p.
PUB TYPE Information Analyses (070) -- Viewpoints (Opinion/Position Papers, Essays, etc.) (120)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS Access to Information; *Computer Networks; Electronic Mail; *Ethics; Futures (of Society); Higher Education; Information Networks; International Cooperation
IDENTIFIERS Computer Crimes; Computer Security; Computer Viruses; *INTERNET

ABSTRACT

Institutions of higher education in the United States are making use of educational communication networks, such as the National Science Foundation's INTERNET system, to enhance research and learning. Such information networks are used to exchange information electronically, and exist not only in the United States, but also in other countries. Privacy and equal access to information are ethical issues that must be considered by those who govern and use computer networks. Security is also necessary to keep data from being erased, changed, plagiarized, or destroyed. The well-publicized damage to INTERNET in 1986 involved breaches of security in university, military, research and development laboratory, and commercial computers. In 1988, INTERNET was again the target, this time of a computer virus planted by a Cornell University (New York) student. Whether networks are used simply for electronic mail purposes, for academic library services, or for international cooperative networks, security, privacy, and equality of access are the major issues to be considered. (33 references) (DB)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☒ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

ED332689

The Future of Electronic Educational Networks: Some Ethical Issues

by

Dell Johnson
May 1991

IR015034

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Dell Johnson

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

BEST COPY AVAILABLE

Dell Johnson

The Future of Electronic Educational Networks: Some Ethical Issues

In the future, institutions of higher learning will be expected to keep themselves up to date by using the power of network communications to enhance research and learning. Future educational networks will evolve from the connections among institutions now using such links as INTERNET and BITNET. Overall increase in the use of National Science Foundation's INTERNET system has risen sevenfold in the past two years, due to improved network systems. Between 1988 and 1993, investments in business local area networks and wide area networks are projected to rise fourteenfold. In 1987 alone, U.S. companies spent $14.7 billion on private networks.1 These figures show how popular the nationwide networks are. Soon international connections will be the norm.

Educators will be concerned with many aspects of constructing and using the inevitable international educational networks. Foremost among their considerations should be the ethical issues of a phenomenon which could link every person on earth into the "global village" predicted by McLuhan. In addition to economic, technological and operational problems, questions concerning security, privacy and equality of access will demand the attention of network planners.

Security is necessary to keep valuable data from being erased, changed, plagiarized, or destroyed by disaster. Privacy is needed to protect personal information concerning faculty and

students from being misused or erased. Another important problem concerns the information "haves" and "have nots." Equality of access to information by all socioeconomic groups is crucial to educational institutions; therefore, a global network of such schools should ensure easy and affordable access to all. These concerns must be addressed by the governing body of an international electronic educational network in order to maintain the ideals which higher education has always attempted to foster.

The necessity for increased levels of computer security has been brought to the world's attention through several incidents during the past few years. Viruses, worms, espionage, vandalism and crime have all affected network users adversely. Tighter security may not be the answer.

The INTERNET has been the target of at least two expensive and well-publicized breaches of security. In 1986 a West German hacker connected to an international gateway and Tymnet used the Lawrence Berkeley Laboratory computer system as a hub. Over a period of 10 months he attacked 450 computers and successfully entered over 30 of them, including universities, military installations, R & D labs and commercial computer companies. He was caught and tried for espionage for selling to the KGB sensitive military data about the SDI (the Star Wars defensive project) and information about how to break into UNIX computers. Due to a 75-cent error in the LBL network accounts, a system operator named Clifford Stoll began to monitor all the hacker's transactions. Although the "wily hacker" was responsible for at least $100,000 in lost computer time, damaged files, and time

spent tracking him, Stoll claims the greater damage was in the violation of trust which the hacker perpetrated. "At the least he was trespassing, invading others' property and privacy; at worst, he was conducting espionage. He broke into dozens of computers, extracted confidential information, read personal mail, and modified system software. He risked injuring medical patients and violated the trust of our network community. Money and time can be paid back. Once trust is broken, the open, cooperative character of our networks may be lost forever."2

Due to his skill at tracking hackers, Stoll was called upon to help identify the person who planted the INTERNET Worm in November 1988. This virus, originating at Cornell University, within hours had infected over 6000 UNIX computers across the US. Many thousands of hours of working time were lost, and damage is estimated to be more than $97 million. This experimental, self-replicating program was created by a computer science graduate student named Robert T. Morris, Jr. and interjected into the INTERNET system. Morris is serving three years' probation, must pay a $10,000 fine and was ordered to perform 400 hours of community service. The network community seems divided on whether the punishment was harsh enough. "Some hackers view RTM as a 'freedom fighter,' but some say he is placing freedom of information at risk [and] many worry about the social implications of computer security [which will] make it difficult for legitimate users to access information."3

Security problems involving viruses and other rogue programs continue to plague the networks. Some vandals are willing to incur great personal expense to fulfill their plans. In the summer of 1990 in the UK, unknown persons packaged and mailed out 10,000 copies of a floppy disk containing a computer virus. Persons who had attended an international conference on AIDS sponsored by the World Health Organization were the targets of this attack, which may have cost the authors of the virus as much as $1 million. Computer networks at medical research facilities in many countries were potentially as risk from this attack, the purpose of which has not been determined.4

Recent estimates of the spread of viruses in the U.S. indicate that by the end of this year "most companies with 400 or more personal computers will have a virus attack once a month if nothing is done to stop the infections."5 Preventive measures include anti-viral programs, programs which alert computer users to the presence of a virus, and not sharing software.

In addition to unauthorized intrusions, network administrators must also secure their systems against damage due to natural disasters, power failures and sabotage. Preventive measures and recovery methods should be carefully planned, since loss of "up" time can be extremely expensive. The Mexico City earthquake caused losses of $1 million per day for Bank of America and its affiliates. A fire in the Hinsdale, Ill. central switching facilities of Bell Co. destroyed fiber and digital circuits supporting over 50,000 lines, disrupting businesses and private transactions for many hours.6 Standby sites and dress

rehearsals for disaster recovery should be included in network planning.

In response to the rising tide of computer crime, Vermont Senator Patrick Leahy sponsored a bill in the fall of 1990 which would stiffen the penalties for computer crimes and distinguish between reckless and intentional crime. Designed to close loopholes in the Computer Fraud and Abuse Act, the bill would try to "find a delicate balance between judicial protection and technological innovation."7 Since experts say that most computer crimes are committed by authorized users, Leahy wants the law to create a deterrent while still avoiding excessive punishments. The Computer Professionals for Social Responsibility agree with Leahy's fear that with no clear guidelines concerning computer crime, law enforcement officials could become overzealous, endangering the freedom of access and privacy of computer users.

Educational networks must also be concerned with the privacy of the persons who use them. Since government agencies are also part of such networks, potential exists for capturing data about students, professors, employees or even groups of people in various "dataveillance" techniques. Such famous authors as Zamyatin, Kafka, Huxley and Orwell have described the potential for tyranny which surveillance provides. Computer networking allows the compilation of information on a person's credit history, tax returns, medical records, educational transcripts, and entertainment choices -- essentially, a life-to-death dossier. There is no guarantee of accuracy of all the data, especially when it is lifted from its proper context. The

Privacy Protection Study Committee has concluded that the "real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, even wholly justifiable."8 People could begin to fear that "every word, deed, purchase, and even thought is to be recorded and available for scrutiny. [How could] a person feel free to worship, speak, associate with others, and think as he pleases?"9

The existing privacy laws were written before technological innovations such as E-mail, communications networks, and cellular telephones. Therefore, network administrators must fill the gap by agreeing on international standards of privacy protection such as a Code of Fair Information Practice, a form of which has been adopted in nearly a dozen foreign countries. Provisions of such a code include: no personal data record-keeping systems whose existence is a secret, individuals must be able to find out what their file contains, must be able to prevent information being used for purposes other than the original intent, must be able to correct any errors, and organizations using such personal information must be responsible for reliability and for preventing misuse of the data.10

A recent incident illustrates the growing concern about misuse of aggregated data. Last fall Lotus Corp. proposed a CD-ROM product called Marketplace: Households which would contain personal data including income level and buying habits of 120 million citizens. None of the persons included were contacted to

verify the data nor was consent sought. Lotus cancelled the project after receiving letters from nearly 30,000 protestors. The major objection to the product was that it is not erasable, so erroneous data could not be corrected. A solution to such a controversy would be the use of ~~consensus~~ by consent information; in fact consumers in the future may even be compensated for the use of their private information.11

The growing concern over network security could result in regulations which would restrict access and interfere with the goals of an international educational network. Proponents of freedom of access claim that hackers serve society by exposing weaknesses in computer networks. An organization called the Electronic Frontier Foundation tries to raise public awareness about civil liberties and first amendment rights for electronic publications. This group has joined with the Computer Professionals for Social Responsibility to promote discussions of civil liberties as they relate to electronic networks. These people consider most hackers as "information freedom fighters."12 There are unresolved legal questions concerning the government's seizure of entire systems, when only some of the files therein are pertinent to the investigation being conducted. Operators of electronic bulletin boards may have certain liabilities, but these too are still hazy. The Electronic Communication Privacy Act seeks to provide protection for private E-mail and directories on bulletin board systems. System owners may even be open to lawsuits if they do not have "adequate security

protection for customer information or for life-threatening operations such as patient monitoring or traffic control."13

The question of freedom of access also includes whether users should be charged a fee for access to the educational networks. Lack of educational opportunity leads to a new division of society, the "information divide." Many information professionals feel that nations cannot afford to allow an "electronic aristocracy" to develop against the "backdrop of spiritual, intellectual and material poverty."14 Society is divided into computer haves and have nots. Access to the international educational network could incur costs comparable to connecting to BITNET, a range of $3000 to $10,000 in 1989, depending on the size of the educational institution. Even access to such a network would not guarantee that all potential users would be able to get the information they need. If they do not have the computer skills themselves and cannot obtain the help of someone who possesses the skills, a "class of people who are already information poor could conceivably be further disenfranchised."15 And there will undoubtedly be institutions, especially in other parts of the world, which will not be able to access any electronic network, due to financial or technological constraints. Libraries and other educational facilities are urged to provide training programs on the use of the networks to "all members of their constituencies...teachers, students and the population in general" to be supported by public or private funds, rather than fees.16 Some libraries will decide that "enhanced" services be paid for by the patron, including those

services such as online or CD-ROM searches, which are time and effort savers rather than the only source of the data.

The development of a world-wide electronic network is already underway. Many issues about the policies governing such a network are still to be decided, including access, security, privacy, the responsibilities and rights of the network administrators, culpability in the case of intruders, and other ethical issues. Most users feel that care must be taken that strengthening security does not hinder free flow of information. The challenge is to preserve the openness characteristic of U.S. academic networks while adopting legal protective measures. "If important technical and policy issues related to security are not handled now in the up-front design rather than after the fact as add-on, we will not have effective security in large new networks, and their integrity and believability will be suspect."17 Professional societies will develop or update codes of ethics and will police themselves to help maintain the open access which is necessary to academic freedom. Educators, computer users and information professionals may decide to institute a licensing authority. If the networks are to be the information highways, then users should be required to pass a test for a "drivers' license." Violations of network regulations could then result in the revoking of licenses, thus denying the misusers their network privileges.

Academic libraries should consider operating in a manner similar to public utilities, where users pay fees large enough to cover the operating expenses. In the U.S. all but the most

poverty-stricken citizens manage to subscribe to electric, telephone, and water utilities and even cable TV. Libraries could offer enhanced services to citizens willing to subscribe to those services. Such services as online searches, telephone reference, electronic publishing, and network access could be included in the information utility concept. Whatever the level of services offered and whether or not direct fees are charged, the electronic educational network must adopt an international focus in connectivity and in resource sharing. The network should offer distance education to underdeveloped regions in the form of health and academic studies. "It may be that tele-education and tele-health are the only hope for breaking the vicious circles that go with exploding population, illiteracy, malnutrition, and lack of jobs... In some ways telepower could even help democratize political practices in modern society."18 Libraries will be central to such educational efforts.

Librarians may expect to be using the educational networks to provide information locally and around the world. They will become teachers, offering bibliographic instruction and guidance to students in using the networks. Through their expertise they will become marketers of their libraries and interpreters of the information scene. They may even be called upon to become professors, teaching classes in information theory and information retrieval to college students. Sometime during their schooling, tomorrow's students must be taught the ethics of computer network usage. Many parents have no background themselves in this area; therefore they cannot properly guide

their children, as they would in telephone behavior for example. Teaching about ethics is considered more effective in the long run than tougher laws and tighter security.19

In a democracy such as we hope the world is becoming, the ethical issues must be given top priority in order that the users-to-be of the electronic educational network will not face a system usurped by totalitarian or anarchistic controllers. Lack of trust would cancel its usefulness as a vehicle for research and education. The ideal situation is a network controlled by an international governing body which is not unduly affected by national politics or adversely affected by economic constraints. Security, privacy and equality of access should be major issues in constructing this global network.

NOTES

1.George Gilder, "Into the Telecosm," **Harvard Business Review** (March-April 1991): 150-161.

2.Clifford Stoll, "Stalking the Wily Hacker," **Communications of the ACM** v 31 n 5 (May 1988): 484-497.

3.Jonathan Littman, "The Shockwave Rider," **PC Computing** v 3 n 6 (June 1990):142-156.

4.Gerard Blanc, "Viruses: A New Form of Crime," **Computing Canada** v 16 n 12 (June 7, 1990): 24.

5."Virus cases multiplying: Heavy PC users expected to be infected every month," **Austin American Statesman** (March 17, 1991):E-1.

6."Disaster Recovery Planning in an Integrated Network Environment," **Datapro Reports on Information Security** (Delran, NJ: McGraw-Hill, 1990).

7.Vanessa Jo Grimm, "Leahy doesn't want officers to go too far," **Government Computer News** v 9 n 18 (Sept. 3, 1990):110-112.

8. Roger A. Clarke, "Information Technology and Dataveillance," **Communications of the ACM** v 31 n 5 (May 1988):498-512.

9. Gene Stephens, "High-Tech Crime: The Threat to Civil Liberties," **The Futurist** (July-Aug. 1990):20-23.

10. Michael Rogers Rubin, "The Computer and Personal Privacy, Part II: The Emerging Worldwide Response to the Threat to Privacy from Computer Databases," **Library Hi Tech** v 6 n 1 (1988):87-96.

11. Peter H. Lewis, "Databases withdrawn, but privacy debate continues," **Austin American Statesman** (April 8, 1991):C-2.

12. Pamela Samuelson, "Is Information Property?" **Communications of the ACM** v 34 n 3 (March 1991):15-18.

13. Dorothy E. Denning, "The United States vs. Craig Neidorf: Debate," **Communications of the ACM** v 34 n 3 (March 1991):23-43.

14. Trevor Haywood, "Electronic information: the withering of public access," **New Horizons for the Information Profession: Meeting the Challenge of Change**. Proceedings of the Annual Conference of the Institute of Information Scientists, University of Warwick, 1987. (London: Taylor Graham, 1988):195-206.

15. Arthur J. Cordell, "Preparing for the Challenges of the New Media," **The Futurist** (March-April 1991):20-24.

16. Timothy M. Ashmore, "Accessing Electronic Information: A Question of Ethics," Paper presented at the meeting of the International Communication Association, San Francisco, CA May 26, 1898. (ED314094):2-8.

17. Lance J. Hoffman and Paul C. Clark, "Imminent Policy Considerations in the Design and Management of National and International Computer Networks," **IEEE Communications** v 29 n 2 (Feb. 1991):68-74.

18. Joseph N. Pelton, "Telepower: The Emerging Global Brain," **The Futurist** (Sept.-Oct. 1989):9-14.

19. "Lessons in ethics might curb computer crime, experts say," **Austin American Statesman** (Mar. 16, 1991):D-2.

Future Electronic Educational Networks:
Some Ethical Issues

Suggested Readings -- BOOKS:

Forester, Tom and Perry Morrison. **Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing**. Cambridge, MA: The MIT Press, 1990.

O'Leary, T.J. and Brian K. Williams. **Computers and Information Systems**. 2 ed. Redwood City, CA: Benjamin Cummings, 1989.

Rochester, Jack B. and John Gantz. **The Naked Computer**. New York: William Morrow, 1983.

Schweitzer, James A. **Computer Crime and Business Information**. New York: Elsevier, 1986.

Stoll, Clifford. **The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage**. New York: Doubleday, 1989.

Van Duyn, J. **The Human Factor in Computer Crime**. Princeton, NJ: Petrocelli, 1985.

ARTICLES:

Ashmore, Timothy M. "Accessing Electronic Information: A Question of Ethics." Paper presented at the meeting of the International Communication Association, San Francisco, CA. May 26, 1989. (ED314094 ERIC).

Clarke, Roger A. "Information Technology and Dataveillance." **Communications of the ACM** 31:5 May 1988: 498-512.

Denning, Dorothy E. "The United States vs. Craig Neidorf" **Communications of the ACM** 34:3 March 1991:23-43.

Haywood, Trevor. "Electronic information: the withering of public access." **New Horizons for the Information Profession: Meeting the Challenge of Change**. Proceedings of the Annual Conference of the Institute of Information Scientists, University of Warwick, 1987. London: Taylor Graham, 1988.

Hoffman, Lance J. and Paul C. Clark. "Imminent Policy Considerations in the Design and Management of National and International Computer Networks." **IEEE Communications** 29:2 Feb. 1991, 68-74.

Samuelson, Pamela. "Is Information Property?" **Communication of the ACM** 34:3 March 1991, 15-18.

Stephens, Gene. "High-Tech Crime: The Threat to Civil Liberties." **The Futurist**. July-Aug. 1990, 20-25.

Stoll, Clifford. "Stalking the Wily Hacker." **Communications of the ACM** 31:5 May 1988, 484-497.